Quantum Conditional Mutual Information, Reconstructed States, and State Redistribution

Fernando G.S.L. Brandão[1], Aram W. Harrow[2], Jonathan Oppenheim[3], Sergii Strelchuk[4]
[1] *Department of Computer Science, University College London*
[2] *Institute for Theoretical Physics, Massachusetts Institute of Technology*
[3] *Department of Physics, University College London*
[4] *Department of Applied Mathematics and Theoretical Physics, University of Cambridge*

SUPPLEMENTAL MATERIAL

A. Auxiliary lemmas

Lemma 1. *If $\pi \leq 2^{\lambda}\sigma$, then $S(\rho||\pi) \geq S(\rho||\sigma) - \lambda$.*

The proof of the lemma follows directly from the operator monotonicity of the log function. □

Lemma 2 is due to Audenaert and Eisert:

Lemma 2 (Theorem 3 of [1])**.** *For all states ρ and σ on a d-dimensional Hilbert space, with $T = \|\rho - \sigma\|_1$ and $\beta = \lambda_{\min}(\sigma)$,*

$$S(\rho||\sigma) \leq T\log(d) + \min\left(-T\log T, \frac{1}{e}\right) - \frac{T\log\beta}{2}. \quad (1)$$

The next lemma is due to M. Piani. It will suffice to state it for the case where $\mathbb{M}$ is the set of all measurements.

Lemma 3. *[Theorem 1 of [2]] Consider two systems X and Y with joint Hilbert space $\mathcal{H}_X \otimes \mathcal{H}_Y$, and a convex reference set K. Suppose the reference set K is such that for all POVM elements M_i and all $\sigma_{XY} \in K$, $\mathrm{tr}_X(M_i^X \sigma_{XY}) \in P$ (up to normalization). Then for every ρ_{XY},*

$$\begin{aligned} &\min_{\sigma_{XY}\in K} S(\rho_{XY}||\sigma_{XY}) \quad (2)\\ \geq\ &\min_{\sigma_X\in K} \mathbb{M}S(\rho_X||\sigma_X) + \min_{\sigma_Y\in K} S(\rho_Y||\sigma_Y). \end{aligned}$$

The following Lemma is due to Fawzi and Renner [3] who stated it in a slightly more general form. It was used in their proof of Eq. (4) in the main text. Below is a very similar, but somewhat shorter, proof.

Lemma 4. *Suppose $\rho_{X^nY^n}$ satisfies $\rho_{X^n} = \tau_{X^n}$ and $[\rho, P_{XY}(\pi)] = 0$ for all $\pi \in \mathcal{S}_n$. Then there exists a measure μ over states σ_{XY} (independent of ρ) with each $\sigma_X = \tau_Y$ and*

$$\rho_{X^nY^n} \leq n^{O(d_X^2 d_Y^2)} \int \sigma^{\otimes n}\mu(d\sigma), \quad (3)$$

where d_X, d_Y are the dimensions of X and Y.

Proof. First purify ρ to a state $|\rho\rangle_{X^nY^nZ^n} \in \mathrm{Sym}^n(XYZ)$ (the symmetric subspace in $(XYZ)^n$) with $d_Z = d_X d_Y$ using Lemma 4.2.2 of [4]. For V an isometry from $X \to YZ$, define

$$|\sigma(V)\rangle_{XYZ} = \frac{1}{\sqrt{d_X}} \sum_{i=1}^{d_X} |i\rangle\, V\, |i\rangle \quad (4)$$

and $\sigma(V) = |\sigma(V)\rangle\langle\sigma(V)|$. Observe that $\sigma(V)_X = \tau_X$. We will show that

$$|\rho\rangle\langle\rho| \leq n^{O(d_X^2 d_Y^2)} \int \sigma(V)^{\otimes n}\mu(d\sigma), \quad (5)$$

which will imply Eq. (3).

Our strategy will be to expand both sides of Eq. (5) in the Schur basis. Schur duality uses the following notation:

$$(\mathbb{C}^d)^{\otimes n} \overset{\mathcal{U}_d\times\mathcal{S}_n}{\cong} \bigoplus_{\lambda\in\mathrm{Par}(n,d)} \mathcal{Q}_\lambda^d \hat{\otimes} \mathcal{P}_\lambda. \quad (6)$$

This is explained in detail in [5], but briefly, $\mathrm{Par}(n,d)$ denotes the set of partitions of n into $\leq d$ parts, $\mathcal{Q}_\lambda^d$ is an irrep of the unitary group $\mathcal{U}_d$, $\mathcal{P}_\lambda$ is an irrep of the symmetric group $\mathcal{S}_n$, $\hat{\otimes}$ means that we interpret the tensor product as an irrep of $\mathcal{U}_d \times \mathcal{S}_n$, and $\overset{\mathcal{U}_d\times\mathcal{S}_n}{\cong}$ means that the isomorphism respects this representation structure. Let U_{Sch} denote the unitary transform realizing the isomorphism in Eq. (6). We can write

$$\begin{aligned} &(U_{\mathrm{Sch}}^X \otimes U_{\mathrm{Sch}}^{YZ})\,|\rho\rangle = \\ &\sum_{\substack{\lambda_1\in\mathrm{Par}(n,d_X)\\ \lambda_2\in\mathrm{Par}(n,d_Y d_Z)}} c_{\lambda_1,\lambda_2}\,|\lambda_1\rangle_X\,|\lambda_2\rangle_{YZ}\,|\chi_{\lambda_1,\lambda_2}\rangle\,|\theta_{\lambda_1,\lambda_2}\rangle\,, \quad (7) \end{aligned}$$

where $\sum_\lambda |c_\lambda|^2 = 1$, $|\chi_{\lambda_1,\lambda_2}\rangle, |\theta_{\lambda_1,\lambda_2}\rangle$ are arbitrary unit vectors in $\mathcal{Q}_{\lambda_1}^{d_X} \otimes \mathcal{Q}_{\lambda_2}^{d_Y d_Z}$ and $\mathcal{P}_{\lambda_1} \otimes \mathcal{P}_{\lambda_2}$ respectively. However, the permutation invariance and Schur's Lemma mean that (following arguments along the lines of Section 6.4.1 of [5]) the only nonzero terms have $\lambda_1 = \lambda_2$ and $|\theta_{\lambda,\lambda}\rangle =: |\Phi_\lambda\rangle$ is the unique permutation-invariant state in $\mathcal{P}_\lambda \otimes \mathcal{P}_\lambda$. Thus we can (using $d_X \leq d_Y d_Z$) rewrite Eq. (7) as

$$(U_{\mathrm{Sch}}^X \otimes U_{\mathrm{Sch}}^{YZ})\,|\rho\rangle = \sum_{\lambda\in\mathrm{Par}(n,d_X)} c_\lambda\,|\lambda\rangle_X\,|\lambda\rangle_{YZ}\,|\chi_\lambda\rangle\,|\Phi_\lambda\rangle\,. \quad (8)$$

To calculate c_λ we use the fact that $\rho_{X^n} = \tau_{X^n}$. Thus measuring the irrep label should yield outcome λ with probability $\dim \mathcal{P}_\lambda \dim \mathcal{Q}_\lambda^{d_X}/d_X^n$, and we have

$$c_\lambda = \sqrt{\frac{\dim \mathcal{P}_\lambda \dim \mathcal{Q}_\lambda^{d_X}}{d_X^n}}. \tag{9}$$

A similar argument implies that

$$(U_{\text{Sch}}^X \otimes U_{\text{Sch}}^{YZ}) \left|\sigma(V)\right\rangle^{\otimes n} = \sum_{\lambda \in \text{Par}(n,d_X)} c_\lambda \left|\lambda\right\rangle_X \left|\lambda\right\rangle_{YZ} \left|\chi_\lambda(V)\right\rangle \left|\Phi_\lambda\right\rangle, \tag{10}$$

for some states $\left|\chi_\lambda(V)\right\rangle$. The coefficients c_λ are the same as in Eq. (9) because $\sigma(V)_{A^n}^{\otimes n} = \tau_{A^n}$. Averaging $\sigma(V)^{\otimes n}$ over all isometries V yields a state that commutes with $(U_X \otimes I_{YZ})^{\otimes n}$ and $(I_X \otimes U_{YZ})^{\otimes n}$ for all $U_X \in \mathcal{U}_{d_X}, U_{YZ} \in \mathcal{U}_{d_Y d_Z}$. Thus

$$(U_{\text{Sch}}^X \otimes U_{\text{Sch}}^{YZ}) \mathop{\mathbb{E}}_V [\sigma(V)^{\otimes n}] (U_{\text{Sch}}^X \otimes U_{\text{Sch}}^{YZ})^\dagger = \sum_{\lambda \in \text{Par}(n,d_X)} |c_\lambda|^2 \left|\lambda,\lambda\right\rangle \left\langle\lambda,\lambda\right| \otimes \tau_{\mathcal{Q}_\lambda^{d_X}} \otimes \tau_{\mathcal{Q}_\lambda^{d_Y d_Z}} \otimes \left|\Phi_\lambda\right\rangle \left\langle\Phi_\lambda\right|. \tag{11}$$

It follows from (8) and (11) that

$$\begin{aligned} \left|\rho\right\rangle \left\langle\rho\right| &\leq (\max_\lambda \dim \mathcal{Q}_\lambda^{d_X} \dim \mathcal{Q}_\lambda^{d_Y d_Z}) \mathop{\mathbb{E}}_V [\sigma(V)^{\otimes n}] \\ &= \binom{d_X + n - 1}{n} \binom{d_Y d_Z + n - 1}{n} \mathop{\mathbb{E}}_V [\sigma(V)^{\otimes n}] \\ &\leq n^{d_X} n^{d_Y d_Z} \mathop{\mathbb{E}}_V [\sigma(V)^{\otimes n}] \\ &= n^{d_X^2 d_Y^2 + d_X} \mathop{\mathbb{E}}_V [\sigma(V)^{\otimes n}]. \end{aligned}$$

□

B. The measured entropy lower bound

To prove the inequality stated in the Eq. (17) of the main text, we first prove the following lemma which is a version of the postselection technique of [6] for quantum operations.

Lemma 5. *For every permutation-invariant quantum operation $\Lambda : B^n \to B^n C^n$ and every state $\pi \in B^n$,*

$$\Lambda(\pi) \leq \text{poly}(n) \int \mathcal{E}^{\otimes n}(\pi) \mu(d\mathcal{E}), \tag{12}$$

where μ is a measure over quantum operations $\mathcal{E} : B \to BC$.

Proof. Since $\Lambda : B^n \to B^n C^n$ is permutation-invariant, it follows that its Jamiolkowski state $J_\Lambda \in \mathcal{D}((\overline{B}^n \otimes B^n \otimes C^n)$ (with $\overline{B} \cong B$) is permutation-invariant. We now apply Lemma 4 in the Supplemental Material to find a distribution μ over $\sigma \in \mathcal{D}(\overline{B} \otimes B \otimes C)$ with

$$J_\Lambda \leq \text{poly}(n) \int \sigma^{\otimes n} \mu(d\sigma), \tag{13}$$

and each $\sigma_{\overline{B}} = \tau_{\overline{B}}$. This latter condition means that each σ can be also thought of as $J_\mathcal{E}$ for some $\mathcal{E} : B \to BC$. We complete the proof using the relation:

$$\begin{aligned} &\text{tr}_{\overline{B}^n}((\pi^T \otimes I_{B^n C^n}) J_\Lambda) \\ &\leq \text{poly}(n) \int \text{tr}_{\overline{B}^n}((\pi^T \otimes I_{B^n C^n}) J_\mathcal{E}^{\otimes n}) \mu(d\mathcal{E}), \end{aligned} \tag{14}$$

and the fact that $\text{tr}_{\overline{B}^n}((\pi^T \otimes I_{B^n C^n}) J_\Lambda) = \Lambda(\pi)/\dim(B)^n$ and $\text{tr}_{\overline{B}^n}((\pi^T \otimes I_{B^n C^n}) J_\mathcal{E}^{\otimes n}) = \mathcal{E}^{\otimes n}(\pi)/\dim(B)^n$. □

We now turn to proving the measured entropy lower bound:

Proposition 6 (Eq. (17) in the main text)**.** *For every state ρ_{BCR} one has*

$$\begin{aligned} &\lim_{n\to\infty} \min_{\Lambda : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda \otimes \text{id}_{R^n}(\rho_{BR}^{\otimes n})) \\ &\geq \min_{\Lambda : B \to BC} \mathbb{M}S(\rho_{BCR} || \Lambda \otimes \text{id}_R(\rho_{BR})). \end{aligned} \tag{15}$$

Proof. For $\Lambda : B^n \to B^n C^n$, define

$$\tilde{\Lambda}(\omega) := \frac{1}{n!} \sum_{\pi \in S_n} P_{BC}(\pi) \Lambda(P_B^\dagger(\pi) \omega P_B(\pi)) P_{BC}(\pi)^\dagger, \tag{16}$$

with $P_X(\pi)$ a representation of a permutation π from S_n (symmetric group of order n) in $X^{\otimes n}$ such that $P_X(\pi) \left|a_1, \ldots, a_n\right\rangle = \left|a_{\pi^{-1}(1)}, \ldots, a_{\pi^{-1}(n)}\right\rangle$. Let Sym be the set of all permutation-invariant quantum operations, i.e. all Λ such that $\Lambda = \tilde{\Lambda}$.

Using Proposition 3 in the main text and the fact that the relative entropy is doubly convex we obtain [7]

$$\begin{aligned} &\lim_{n\to\infty} \min_{\Lambda : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda \otimes \text{id}_{R^n}(\rho_{BR}^{\otimes n})) \\ &\geq \lim_{n\to\infty} \min_{\substack{\Lambda : B^n \to B^n R^n \\ \Lambda \in \text{Sym}}} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda \otimes \text{id}_{R^n}(\rho_{BR}^{\otimes n})). \end{aligned}$$

Lemma 5 gives that for every $\Lambda_n : B^n \to B^n C^n \in$ Sym,

$$\begin{aligned} &(\Lambda_n \otimes \text{id}_{R^n})(\rho_{BR}^{\otimes n}) \\ &\leq \text{poly}(n) \int (\mathcal{E} \otimes \text{id}_R(\rho_{BR}))^{\otimes n} \mu_n(d\mathcal{E}), \end{aligned} \tag{17}$$

with $\mu(d\mathcal{E})$ a measure over quantum operations $\mathcal{E} : B \to BC$. Using the previous equation and the operator monotonicity of the log (see Lemma 1 above),

$$\begin{aligned} &\lim_{n\to\infty} \min_{\Lambda : B^n \to B^n C^n} \frac{1}{n} S(\rho_{BCR}^{\otimes n} || \Lambda \otimes \text{id}_{R^n}(\rho_{BR}^{\otimes n})) \\ &\geq \lim_{n\to\infty} \min_{\mu_n} \frac{1}{n} S\left(\rho_{BCR}^{\otimes n} \,\|\, \int (\mathcal{E} \otimes \text{id}_R(\rho_{BR}))^{\otimes n} \mu_n(d\mathcal{E})\right). \end{aligned} \tag{18}$$

To complete the proof we make use of Lemma 3 above. Consider the state $\rho_{BCR}^{\otimes n}$ and let X be the first

copy of ρ_{BCR} in the tensor product and Y the remaining $\rho_{BCR}^{\otimes n-1}$. Define

$$K = \bigcup_{k\in\mathbb{N}} \left(\text{conv}\{(\mathcal{E}\otimes \text{id}_R)(\rho_{BR})^{\otimes k} \ : \ \mathcal{E} : B \to BC\}\right), \tag{19}$$

i.e. the convex hull of tensor products of reconstructed states. It is easy to check that K satisfies the assumption of Lemma 3 above. Therefore:

$$\begin{aligned} &\min_{\mu_n} S\left(\rho_{BCR}^{\otimes n} \parallel \int (\mathcal{E}\otimes \text{id}_R(\rho_{BR}))^{\otimes n}\mu_n(d\mathcal{E})\right) \qquad (20)\\ \geq\ &\min_{\mu} \mathbb{M}S\left(\rho_{BCR} \parallel \int (\mathcal{E}\otimes \text{id}_R(\rho_{BR}))\mu(d\mathcal{E})\right)\\ +\ &\min_{\mu_{n-1}} S\left(\rho_{BCR}^{\otimes n-1} \parallel \int (\mathcal{E}\otimes \text{id}_R(\rho_{BR}))^{\otimes n-1}\mu_{n-1}(d\mathcal{E})\right). \end{aligned}$$

Iterating the equation above n times gives Eq. (15). □

[1] K. M. R. Audenaert and J. Eisert. Continuity bounds on the quantum relative entropy. *J. Math. Phys.*, 46(10):–, 2005, {\ttfamilyarXiv:quant-ph/0503218}.

[2] M. Piani. Relative entropy of entanglement and restricted measurements. *Phys. Rev. Lett.*, 103:160504, Oct 2009, {\ttfamilyarXiv:0904.2705}.

[3] O. Fawzi and R. Renner. Quantum conditional mutual information and approximate markov chains, 2014, {\ttfamilyarXiv:1410.0664}.

[4] R. Renner. *Security of quantum key distribution*. PhD thesis, ETHZ, Zurich, 2005, {\ttfamilyarXiv:quant-ph/0512258}.

[5] A. W. Harrow. *Applications of coherent classical communication and Schur duality to quantum information theory*. PhD thesis, M.I.T., Cambridge, MA, 2005, {\ttfamilyarXiv:quant-ph/0512255}.

[6] M. Christandl, R. Koenig, and R. Renner. Post-selection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, 2009, {\ttfamilyarXiv:0809.3019}.

[7] In more detail: $S(\rho_{BCR}^{\otimes n}||\Lambda(\rho_{BR}^{\otimes n})) = \mathbb{E}_{\pi\in S_n} S(P_{CBR}^{\pi}\rho_{BCR}^{\otimes n}(P_{CBR}^{\pi})^{\dagger}||P_{CBR}^{\pi}\Lambda((P_{BR}^{\pi})^{\dagger}\rho_{BR}^{\otimes n}P_{BR}^{\pi})(P_{CBR}^{\pi})^{\dagger}) = \mathbb{E}_{\pi\in S_n} S(\rho_{BCR}^{\otimes n}||P_{CB}^{\pi}\Lambda((P_{B}^{\pi})^{\dagger}\rho_{BR}^{\otimes n}P_{B}^{\pi})(P_{CB}^{\pi})^{\dagger}) \geq S\left(\rho_{BCR}^{\otimes n}||\ \mathbb{E}_{\pi\in S_n} P_{CB}^{\pi}\Lambda((P_{B}^{\pi})^{\dagger}\rho_{BR}^{\otimes n}P_{B}^{\pi})(P_{CB}^{\pi})^{\dagger}\right)$, with $P_{CBR}^{\pi} := P_{CBR}(\pi)$.